BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: ltfisher@bursor.com

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

M.D., O.F., and J.P., individually and on behalf of all others similarly situated,

Plaintiffs,

v.

GOOGLE LLC and META PLATFORMS, INC.,

Defendants.

Case No. 3:24-cv-06369-AMO

PLAINTIFFS' OPPOSITION TO DEFENDANT META PLATFORMS, INC.'S MOTION TO DISMISS FIRST AMENDED CLASS ACTION COMPLAINT

Hearing: July 10, 2025
Time: 2:00 p.m.
Location: Courtroom 10—19th Floor
Judge: Hon. Araceli Martínez-Olguín

TABLE OF CONTENTS

PAGE(S)

TABLE OF AUTHORITIES

PAGE(S)

CASES

STATUTES

RULES

REGULATIONS

I. INTRODUCTION

Plaintiffs M.D., O.F., and J.P. (collectively "Plaintiffs") hereby oppose Defendant Meta Platforms, Inc.'s ("Defendant" or "Meta") Motion to Dismiss the First Amended Class Action Complaint (ECF No. 37) ("MTD"). Plaintiff M.D. plausibly states a claim under the California Invasion of Privacy Act ("CIPA") § 631(a) and § 632 and for invasion of privacy because Defendant intentionally, and without the consent of Plaintiffs and class members, intercepted sensitive and confidential health communications between Plaintiffs (and class members) and third party Dermacare, LLC d/b/a BlueChew ("BlueChew"), via the BlueChew website, www.bluechew.com (the "Website"). Plaintiff O.F. states a claim under the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. § 5701, *et seq.* ("WESCA") based on the same conduct. Plaintiff J.P. states a claim under the Maryland Wiretapping and Electronic Surveillance Act, Md. Code, Cts. & Jud. Proc. Code Sec. 10-401, *et seq*. ("MWESA") based on the same conduct.

BlueChew is an online health platform wherein registered users connect with health care providers for the diagnosis and treatment of erectile dysfunction. Through the Website, users, such as Plaintiffs and class members, fill out a medical questionnaire and, if they qualify, purchase erectile dysfunction medication. While Plaintiffs and class members reasonably believed and expected that their communications with BlueChew regarding these sensitive health issues would be kept confidential, they were not. That is because BlueChew embedded Defendant's software on its Website, the Facebook Tracking Pixel, which captured Plaintiffs' and class members' interactions with the Website—including their personal information and information regarding the erectile dysfunction medications they purchased—and transmitted said health information to Defendant. Defendant then used this information for its own benefit by incorporating it into its advertising machinery which functioned to place Plaintiffs and class members into targeted audiences for advertisers of similar medications. Indeed, Plaintiffs in this case were retargeted and subject to advertising for erectile dysfunction medications because of Defendant's use of their confidential health information. Defendant makes the Facebook Tracking Pixel free for website owners to use for exactly that reason, so that it can receive valuable information from website interactions and then generate highly specific audience segments which it then uses to sell advertising. However, where,

as here, protected health information is surreptitiously transmitted to Defendant without the consent of Plaintiffs and class members, it is unlawful.

As a result of Defendant's unlawful conduct, Plaintiff M.D. brings the present action on behalf of himself and "all natural persons in California who, during the class period, purchased medication on www.bluechew.com." *See* First Amended Class Action Complaint (ECF No. 34) ("FAC"), ¶ 78. Plaintiff O.F. brings claims on behalf of himself and an identical class of persons in Pennsylvania. *Id.* ¶ 79. Plaintiff J.P. brings claims on behalf of himself and an identical class of persons in Maryland. *Id.* ¶ 80.

Defendant now moves to dismiss Plaintiffs' claims. However, courts have rejected similar motions to dismiss in other cases involving the Facebook Tracking Pixel, including in *Rickwalder v. Meta Platforms, Inc*., 2022 WL 22462351 (Cal. Super. Ct. Sept. 15, 2022), *Yoon v. Meta Platforms, Inc.*, 2024 WL 5264041 (N.D. Cal. Dec. 30, 2024), and *Gershzon v. Meta Platforms, Inc.*, 2023 WL 5420234, at *1 (N.D. Cal. Aug. 22, 2023). *See also St. Aubin v. Carbon Health Techs., Inc.*, 2024 WL 4369675, at *3 (N.D. Cal. Oct. 1, 2024) (rejecting similar arguments where the Facebook Tracking Pixel was used to intercept health information). For the reasons set forth herein, the Court should deny Defendant's motion to dismiss.

II. STATEMENT OF FACTS

BlueChew's Website allows registered users to connect with health care providers for the diagnosis and treatment of erectile dysfunction. FAC ¶ 2; ¶¶ 19-20, Figure 1. The Website offers patients discrete access to prescription erectile dysfunction medications. *Id.* In using the Website, Plaintiffs and class members provided protected health information to BlueChew for the purpose of obtaining medical treatment, including providing responses to a "medical profile" questionnaire to determine whether they qualify for erectile dysfunction medication. *Id.* ¶¶ 20-24, Figures 1-4. Plaintiffs and class members purchased erectile dysfunction medications. *Id.*

Despite being protected by federal and state law, and unbeknownst to Plaintiffs and Class Members, Defendant intercepted their sensitive health information conveyed through the Website using its Facebook Tracking Pixel, and other similar software. The data intercepted and collected included de-anonymized, prescription erectile dysfunction medications purchased by Plaintiffs and

class members on the Website. *Id.* ¶¶ 3-4, 35, 39 (illustrating how the Facebook Tracking Pixel functions to intercept private health information from the Website). Plaintiffs' protected health information that Defendant intercepted was personally identifiable and Defendant used Plaintiffs' and class members' intercepted health information for its own benefit, namely for the purpose of targeted advertising. *Id.* ¶¶ 5, 36, 57 (after intercepting Plaintiffs' and class members protected health information, Defendant processed, analyzed, and assimilated it into datasets like Core Audiences and Custom Audiences (i.e. its proprietary advertising algorithms)). Examples of Defendant's interceptions from the Website clearly show that Defendant intercepted personally identifying information such as name, state of residence, email address, and various forms of protected health information. For example, Defendant intercepted information showing that the BlueChew user registered on the Website, added a medication to their cart, and ultimately purchased the medication. *Id.* ¶ 40, Figures 4 and 5; *see also id.* ¶ 41 ("Through the Facebook Tracking Pixel, Defendant Facebook intercepted and recorded "AddToCart" and "CompleteRegistration" events, which detail information about which prescription the patient was purchasing on the Website."); ¶¶ 42-44. Regardless of whether Plaintiffs and class members are Facebook users, Defendant can match their prescription information to their identity using the personally identifying information they conveyed to BlueChew that was intercepted by Defendant. *Id.* ¶ 56.

At no point during the checkout process on the Website were Plaintiffs and class members alerted that information related to their prescription medications was being intercepted by Defendant. *Id.* ¶ 25. At all relevant times, Plaintiffs and class members had a reasonable expectation of privacy as to the protected health information they transmitted to BueChew because they reasonably believed the communications were between them and BlueChew, and they did not consent to Defendant's interception of their private health information. *Id.* ¶ 6; *see also id.* ¶ 13 (Defendant "committed the interceptions at issue without Plaintiffs' knowledge, consent, or express written authorization."), *id.* ¶¶ 58, 93.

Plaintiff M.D. is a California citizen who, on December 6, 2022, and January 4, 2023, was prescribed and ordered Sildenafil erectile dysfunction medication through the Website. *Id.* ¶ 7. Unbeknownst to Plaintiff M.D., Defendant intercepted his protected health information related to his

prescription medication using the Facebook Tracking Pixel. *Id.* In addition to information related to his prescription medication, Defendant also intercepted Plaintiff M.D.'s personally identifiable information, including his first and last name, email address, and date of birth. *Id.* ¶ 8. Subsequently, because of Defendant's conduct, Plaintiff M.D. has received targeted advertisements relating to erectile dysfunction medications. *Id.* Plaintiff O.F., a Pennsylvania citizen, and Plaintiff J.P., a Maryland citizen, make identical allegations to those of Plaintiff M.D. *Id.* ¶¶ 9-12. Plaintiffs did not discover Defendant's surreptitious intereception of their personal health information until September 2024. FAC ¶¶ 7, 9, 11. For its part, Defendant knew that the incorporation of its software onto the Website would result in its interception of protected health information and personally identifying information of Plaintiffs and class members. *Id.* ¶ 15. As demonstrated by the continued incorporation of the Facebook Tracking Pixel on the Website, Defendant intends to intercept this protected and sensitive health data due to the value it holds for targeted advertising. *Id.* ¶ 94.

III. ARGUMENT

A. Plaintiffs Adequately Allege Intent

Defendant argues that "[a]ll of Plaintiffs' claims fail out of the gate because Plaintiffs fail to allege that Meta intentionally or willfully intercepted their allegedly sensitive information—as each claim requires." MTD at 9. That is wrong.

Interceptions are deemed to be intentional if the defendant is aware that the information it is intercepting may be confidential. *See In re Meta Pixel Tax Filing Cases*, 724 F.Supp.3d 987, 1002-03 (N.D. Cal. Mar. 25, 2024) (finding allegations that Meta intended to intercept confidential tax filing information were sufficient); *Smith v. Google, LLC*, 735 F.Supp.3d 1188, 1198 (N.D. Cal. June 3, 2024) (same). "[I]nterceptions may [also] be considered intentional where a defendant is aware of the defect causing interception and takes no remedial action." *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 815 (N.D. Cal. 2020); *see also Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1044 (N.D. Cal. 2014) (collecting cases). While *In re Google Assistant Priv. Litig.* involved a claim under the federal Wiretap Act, CIPA applies the same standard. *M.G. v. Therapymatch, Inc.*, 2024 WL 4219992, at *3 (N.D. Cal. Sept. 16, 2024) (Martínez-Olguín, J.) ("The analysis for a violation of CIPA is the same analysis for a violation of the federal Wiretap Act."); *see also Brodsky v. Apple*

Inc., 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020); *Yoon*, 2024 WL 5264041, at *4. For CIPA § 632(a), the statute punishes "a person who intends to make a recording of a confidential communication." *Rojas v. HSBC Card Servs. Inc.*, 20 Cal. App. 5th 427, 435 (2018) (internal quotation marks and citation omitted). The standard under MWESA is similar to CIPA, as the "willfulness *mens rea* does not require a showing of 'bad motive' or 'knowing unlawfulness'"; instead, "[i]t is sufficient to show that there was an intentional, rather than inadvertent or negligent, interception." *Holmes v. State*, 236 Md. App. 636, 649 (2018) (quoting *Deibler v. State*, 365 Md. 185, 199 (2001)). Like CIPA, "WESCA is Pennsylvania's state law equivalent to the Federal Wiretap Act." *Ingrao v. AddShoppers, Inc.*, 2024 WL 4892514, at *12 (E.D. Pa. Nov. 25, 2024); *see also Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 125–26 (3d Cir. 2022) (WESCA "operates in conjunction with and as a supplement to the Federal Wiretap Act, 18 U.S.C. § 2510 *et seq.*, which provides uniform minimum protections for wire, electronic, or oral communications."). Therefore, the intent analysis under CIPA and WESCA is the same.

As a threshold matter, "[w]hether a person possesses the requisite intent under CIPA is generally a question of fact." *Gladstone v. Amazon Web Servs., Inc.*, 739 F. Supp. 3d 846, 859 (W.D. Wash. 2024); *see also Smith v. Google, LLC*, 735 F. Supp. 3d 1188, 1198 (N.D. Cal. 2024) ("While Google argues that judicially noticeable policy documents suggest that Google did not actually want to receive personally identifiable information and expressly prohibited developers from transmitting such data, this presents a question of fact that the Court cannot resolve at this stage."); *Hudson v. Superior Ct.*, 7 Cal. App. 5th 1165, 1171 (2017) ("[A] person's intent is a question of fact to be determined from all the circumstances of the case, and usually must be proven circumstantially." (internal citations omitted)). Pennsylvania courts have reached the same conclusion. *United States v. Fumo*, 628 F. Supp. 2d 573, 592 (E.D. Pa. 2007) ("Intent is a question of fact, to be determined by a jury.").

Here, Plaintiffs adequately allege knowledge and intent under each applicable cause of action. *See* FAC ¶¶ 5, 15, 94, 96, 115, 125-26, 137. Plaintiffs allege the Facebook Tracking Pixel is designed for the purpose of recording and analyzing communications between Defendant's customers (like BlueChew) and consumers (like Plaintiffs and class members). *Id.* ¶¶ 26-58; *see*

also Gladstone, 739 F. Supp. 3d at 860 (finding intent element under CIPA § 631(a) and § 632(a) satisfied where "[t]he SAC alleges that Amazon Connect is designed for the purpose of recording and analyzing communications between its customers (like Capital One) and consumers or other entities"). Defendant also knew the Facebook Tracking Pixel may intercept "sensitive" data as evidenced by Meta's Business Tools Terms, which specifically acknowledges that the Facebook Tracking Pixel could be configured to share "health" information with Facebook. *See* MTD at 5. Defendant's knowledge is further gleaned from its role as a defendant in other litigations where the Business Tools, including the Facebook Tracking Pixel, have been used to intercept and transmit information. *Rickwalder, et al. v. Meta Platforms, Inc.*, Case No. 21-cv-383231 (Ca. Super. Ct., Santa Clara Cnty. Mar. 9, 2022); *In Re Meta Pixel Healthcare Litigation*, Docket No. 3:22-cv-03580 (N.D. Cal. June 17, 2022); *Forrest v. Meta Platforms, Inc.*, Docket No. 5:22-cv-03699 (N.D. Cal. June 23, 2022); *Doe v. Meta Platforms, Inc.*, Docket No. 3:22-cv-04680 (N.D. Cal. Aug. 15, 2022); *Doe v. Meta Platforms, Inc.*, Docket No. 3:22-cv-04963 (N.D. Cal. Aug. 30, 2022); *In Re Meta Pixel Tax Filing Cases*, Docket No. 5:22-cv-07557 (N.D. Cal. Dec. 1, 2022).

Despite being aware that the Facebook Tracking Pixel routinely intercepts confidential information, Defendant has failed to take remedial action to prevent such interceptions, including in this case. That is intentional. Defendant is fully aware of the value such protected information holds and intends to intercept it to feed it into its advertising machinery. Defendant has also failed to destroy the protected health information it received from Plaintiffs, evidencing intent. *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d at 827–28 ("[T]he Court finds that Defendants' failure to rectify the defect causing 'false accepts' or destroy the recordings produced under such circumstances could plausibly be considered 'intentional' rather than 'a result of accident or mistake.'"). On the contrary, Defendant has affirmatively *used* the protected health information it intercepted via the Facebook Tracking Pixel to improve its advertising machinery and generate revenue. FAC ¶¶ 5, 36, 57. Indeed, Plaintiffs were targeted with similar advertisements promoting erectile dysfunction medications after visiting the Website. *Id.* ¶¶ 8, 10, 12. In short, Defendant's interception of Plaintiffs' and class members' confidential health information was no accident, it was

intended by Defendant. Otherwise, Defendant would not have used the intercepted confidential information to power its own algorithms and advertising products to derive a profit. *Id.* ¶¶ 5, 36, 57.

Defendant further argues that its Business Tools Terms exonerate it from liability. MTD at 12. But this argument has been squarely rejected in other similar cases. In *Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064 (N.D. Cal. 2023) ("*Meta*"), *motion to certify appeal denied*, 2024 WL 4375776 (N.D. Cal. Oct. 2, 2024), the court found:

> While plaintiffs acknowledge that Meta may tell third parties and Facebook users that it intends to prevent receipt of sensitive health information, plaintiffs contend that is not what Meta really intends. . . What Meta's true intent is, what steps it actually took to prevent receipt of health information, the efficacy of its filtering tools, and the technological feasibility of implementing other measures to prevent the transfer of health information, all turn on disputed questions of fact that need development on a full evidentiary record. . . At this stage, intent has been adequately alleged.

Id. at 1076; *see also In re Meta Pixel Tax Filing Cases*, 724 F. Supp. 3d at 1003 (same).

The same analysis applies here. Defendant acts contrary to its stated position in its Business Tools terms by collecting sensitive data by the means set forth above. *See In re Meta Pixel Tax Filing Cases*, 724 F. Supp. 3d 987, 1003 (N.D. Cal. 2024) ("Meta argues that it could not have intended to receive the information at issue because its Business Tools Terms forbid developers from sending sensitive information to Meta and require that developers have all necessary rights and permissions to lawfully share whatever information they send. . . [T]he Court cannot conclude from their mere existence that Meta and developers intended to or did comply with the terms rather than deviating from them to their mutual benefit."). Defendant's intent is, at minimum, a question of fact. *Id.*; *Gladstone*, 739 F. Supp. 3d at 860 ("Defendant points out that it contractually requires companies that use Amazon Connect to provide notice and obtain consent from their customers . . . but the Court is not convinced that [Defendant's] inclusion of a catch-all provision requiring its customers to comply with the law generally is enough to satisfy its legal obligations under CIPA.") (cleaned up).

Defendant argues that "it was *BlueChew*, not Meta, that chose to install the [Facebook Tracking] Pixel on its website and configured it to transmit particular data." MTD at 10-11. But as

stated above, Defendant obtained and used the intercepted health information for its own benefit, which strongly evidences intent. FAC ¶¶ 5, 36, 57.

Defendant cites to *Doe I v. Google LLC*, 741 F. Supp. 3d 828, 836 (N.D. Cal. 2024) ("*Google*"), where the court granted a motion to dismiss because the plaintiffs' allegations were "too vague to support an inference that the providers have, contrary to [Google's] admonition [not to use the pixel to transmit health information], caused Google to receive the plaintiffs' personal health information" and that the plaintiffs did not "adequately allege that Google intends to receive this information, or that Google intends to feed the information into its own advertising machinery." *Id.* at 836. But numerous other cases in this District have correctly departed from the reasoning in *Google* with regard to the Facebook Tracking Pixel. *See Meta*, 690 F. Supp. 3d at 1076; *In re Meta Pixel Tax Filing Cases*, 724 F. Supp. 3d at 1003 (N.D. Cal. 2024) ("Meta's argument presents a question of fact that the Court cannot resolve at this stage. Whatever agreements may have been in place, those agreements do not establish as a matter of law that Meta did not intend to receive the information plaintiffs claim was transmitted."); *Gershzon v. Meta Platforms, Inc.*, 2023 WL 5420234, at *11 (N.D. Cal. Aug. 22, 2023) (finding intent met with regard to implementation of the Facebook Tracking Pixel and rejecting many of the same arguments raised by Defendant here).

The weight of authority favors Judge Orrick's analysis in *Meta*, which this Court should apply here. Even if this Court were to decline to follow the factually analogous cases involving the same technology (*Meta*, *In re Meta Pixel Tax Filing Cases*, and *Gershzon*), and instead follow the decision in *Google*, it is distinguishable. In *Google*, there was no allegation that "Google intends to feed the information into its own advertising machinery." 741 F. Supp. 3d at 836. Here, Plaintiffs allege that Defendant knowingly receives the confidential health information from BlueChew and integrates it into its proprietary advertising products (such as Core and Custom Audiences) to make them more compelling for advertisers (and thereby to derive a profit). FAC ¶¶ 5, 27 (Defendant generates nearly all its revenue by selling advertising); *id.* ¶¶ 36, 57.

Lastly, contrary to Defendant's assertion (MTD at 10), there is no intent element regarding a claim for invasion of privacy under the California constitution. "[T]he elements of the California constitutional claim for invasion of privacy are: (i) the identification of a specific, legally protected

privacy interest; (ii) a 'reasonable expectation of privacy on plaintiff's part'; and (iii) a sufficiently serious invasion." *Planned Parenthood Fed'n of Am., Inc. v. Ctr. for Med. Progress*, 214 F. Supp. 3d 808, 846 (N.D. Cal. 2016), *aff'd*, 890 F.3d 828 (9th Cir. 2018), *amended*, 897 F.3d 1224 (9th Cir. 2018), and *aff'd*, 735 F. App'x 241 (9th Cir. 2018). Even if there were an intent requirement, for the reasons set forth herein, Defendant acted intentionally because it knew that the Facebook Tracking Pixel was being used to intercept confidential health information and failed to take appropriate remedial action to prevent such disclosures (or destroy health information received from Plaintiffs). Defendant instead used the protected health information to improve its advertising products and generate revenue. FAC ¶¶ 5, 36, 57.

B. Plaintiffs Did Not Consent to The Interception of Their Private Health Information

Defendant argues that "Plaintiffs consented to BlueChew's transmission of information about their activity on its website to service providers like Meta." MTD at 13. That is wrong.

"On a motion to dismiss, the burden of proof to show consent rests with defendants." *Doe v. FullStory, Inc.*, 712 F. Supp. 3d 1244, 1253 (N.D. Cal. 2024); *Meta*, 690 F. Supp. 3d at 1077-78 ("On this motion to dismiss, the issue of consent is front and center and the burden of proof to show this exemption applies is on Meta."); *In re Google RTB Consumer Priv. Litig.*, 606 F. Supp. 3d 935, 949 (N.D. Cal. 2022) ("Google next claims there was lawful consent from both the account holder and the websites. Google bears the burden of proof on consent."). Here, Plaintiffs allege they did not consent to Defendant's interception of their confidential health information conveyed to BlueChew. FAC ¶ 6; *see also id.* ¶ 13 (Defendant "committed the interceptions at issue without Plaintiffs' knowledge, consent, or express written authorization."), *id.* ¶¶ 58, 93. Nevertheless, Defendant argues that Plaintiffs consented based on Blue Chew's purported Privacy Policy.

Before addressing the substance of the purported Privacy Policy, there are several issues that prevent dismissal. First, Plaintiffs do not reference the BlueChew Privacy Policy in the FAC and specifically allege that at "no point during the checkout process are patients alerted that information related to their prescription medication is being intercepted by third parties." FAC ¶ 25. As such, Defendant's argument, which improperly relies on documents extraneous to the pleadings, is belied

by Plaintiffs' allegations. *Smith*, 735 F. Supp. 3d at 1196 ("Although these documents suggest that plaintiffs *could* have consented to Google's alleged data collection, plaintiffs specifically allege that they did not. The mere existence of various terms of service and privacy policies cannot establish at this stage, where the Court must draw all reasonable inferences in plaintiffs' favor, that any of the plaintiffs *did* in fact consent. Google's consent arguments do not provide a basis to dismiss the Section 631 claim.").

Second, even if this Court were to consider the purported BlueChew Privacy Policy, there is a question of fact as to whether its terms are binding on Plaintiffs. Plaintiff O.F. alleges he purchased medication from Blue Chew in January 2022. FAC ¶ 9. Defendant does not append any document showing what the BlueChew sign up screen looked like in January 2022, it only appends the purported sign-up page on February 3, 2021, almost a year before O.F. purchased the medication. Declaration of Melanie M. Blunschi In Support of Defendant Meta Platforms, Inc.'s Motion to Dismiss First Amended Class Action Complaint (ECF No. 38) ("Blunschi Dec."), ¶ 6. Further, even assuming the purported sign-up page on February 3, 2021 was what Plaintiff O.F. was confronted with when he purchased his medication in January 2022, the reference to the terms and conditions is in small print *below* the button to "Create Account." Blunschi Dec., Ex. 5. The Ninth Circuit has held that such a page layout is insufficient to establish mutual assent. *Berman v. Freedom Fin. Network, LLC*, 30 F.4th 849, 858 (9th Cir. 2022) ("We conclude that the design and content of the webpages Hernandez and Russell visited did not adequately call to their attention either the existence of the terms and conditions or the fact that, by clicking on the 'continue' button, they were agreeing to be bound by those terms. The district court properly denied defendants' motion to compel arbitration because an enforceable agreement to arbitrate was never formed."); *see also Sadlock v. Walt Disney Co.*, 2023 WL 4869245, at *10 (N.D. Cal. July 31, 2023); *Yoon*, 2024 WL 5264041, at *4 ("Defendant has not shown that Plaintiffs had the requisite actual or constructive knowledge of the policies."); *id.* ("It is not sufficient to simply allege that the policies exist . . . to prove consent").

The same problem exists for Plaintiffs M.D. and J.P. For Plaintiff M.D., he made purchases from BlueChew on December 6, 2022 and January 4, 2023, but Defendant fails to provide the alleged sign-up screen for either of those dates; instead, Defendant attaches what it purports to be the sign-

up screen on October 8, 2022. Blunschi Dec., ¶ 8. Therefore, there is a question of fact as to what the sign-up screen looked like on the dates in question. Even assuming that the purported sign-up page on October 8, 2022 was what Plaintiff M.D. was confronted with when he purchased his medications on December 6, 2022 and January 4, 2023, there is still a lack of mutual assent because the reference to the purported Terms and Conditions is in small print well below the button to "Create Account" (and below several other links to sign in using a third-party service). Blunschi Dec., Ex. 7; *see also Berman*, 30 F.4th at 858; *Sadlock*, 2023 WL 4869245, at *10. For Plaintiff J.P., he purchased medication from Blue Chew on August 3, 2024, but Defendant fails to provide the alleged sign-up screen on that date; instead, Defendant attaches what it alleges to be the sign-up screen on March 29, 2023, well over a year before Plaintiff J.P.'s purchase. Blunschi Dec., ¶ 9. Even assuming that the purported sign-up page on March 29, 2023 was what Plaintiff J.P. was confronted with when he purchased his medication on August 3, 2024, the reference to the terms and conditions is in small print below the button to "Create Account." Blunschi Dec., Ex. 8. As such, mutual assent is lacking. *Berman*, 30 F.4th at 858; *Sadlock*, 2023 WL 4869245, at *10. Additionally, none of the BlueChew webpages submitted by Defendant even reference or hyperlink the Privacy Policy, further undermining any argument of mutual assent.

The same flaw exists for the Terms and Conditions and Privacy Policies themselves, as none of the versions appended by Defendant match the dates or even the month that Plaintiffs made their purchases. *See* Blunschi Dec., ¶¶ 11-20. Thus, there are questions of fact as whether any BlueChew terms are applicable to Plaintiffs, let alone whether Defendant is permitted to enforce them.

Further, the alleged BlueChew documents have not been properly authenticated. Defendant's counsel cannot authenticate the third-party BlueChew documents. *See* Federal Rule of Evidence 901(a); *In re TikTok, Inc. In-App Browser Priv. Litig.*, 2024 WL 4367849, at *9 (N.D. Ill. Oct. 1, 2024) ("Although the consent defense is, thus, fairly before the court at this stage, the court concludes, for now, that Defendants' submissions are too limited to allow a definitive ruling on the merits of that defense. As an initial matter, the authenticity of the submissions is disputed: Plaintiffs argue that Defendants must verify them . . .").

Even if properly authenticated and binding, BlueChew's purported Privacy Policy does not

establish consent because it did not "explicitly notify" Plaintiffs of the practice at issue. *See Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 620 (N.D. Cal. 2021) ("In order for consent to be actual, the disclosures must 'explicitly notify' users of the practice at issue."); *In re Google Inc.*, 2013 WL 5423918, at *13 (N.D. Cal. Sept. 26, 2013) ("Google points to its Terms of Service and Privacy Policies, to which all Gmail and Google Apps users agreed, to contend that these users explicitly consented to the interceptions at issue. The Court finds, however, that those policies did not explicitly notify Plaintiffs that Google would intercept users' emails for the purposes of creating user profiles or providing targeted advertising."); *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 848 (N.D. Cal. 2014) ("However, as discussed above in the context of express consent, any consent with respect to the processing and sending of messages itself does not necessarily constitute consent to the specific practice alleged in this case—that is, the scanning of message content for use in targeted advertising.").

Indeed, BlueChew's Privacy Policy states the *opposite*—that it safeguards sensitive health information and only shares it with certain enumerated third parties for certain purposes which do not include Meta or online advertising. Ex. 17 p.3-4. The Privacy Policy states:

> **Personally Identifiable Information**
> BLUECHEW may share information about you, including health information and other information that personally identifies you, as follows:
> - with healthcare providers with whom you are connected via BLUECHEW for the provision of their healthcare services to you;
> - with pharmacies, to fulfill prescriptions from your healthcare providers and coordinate medication orders;
> - with service providers that we use to support the Websites or otherwise in connection with administering and providing our Services, and billing and collections, including without limitation any third party payment processor;
> - with other third parties as we deem appropriate or necessary to comply with applicable laws or legal process, such as in response to a subpoena in compliance with applicable privacy laws, or to enforce our Terms and Conditions;
> - to a buyer or successor in the event of a sale, merger or other transaction that involves the transfer of such information to the other company.

Blunschi Dec., Ex. 17 p.3. None of these enumerated scenarios remotely describe the conduct at issue in this case. Defendant seeks to shoehorn this unconsented-to conduct into the "service providers that we use to support the Websites" bullet point, above. However, that bullet point refers to "third party payment processors" and "billing and collections"; it makes no reference to disclosure of private health information to Meta for the purposes of online advertising. Nor can the Facebook Tracking Pixel be reasonably construed to be connected to "administering and providing" health services. The law requires explicit notification, not attenuated, unsupported suppositions Defendant is making here. The BlueChew Privacy Policy falls far short of providing explicit notification of the conduct at issue. This is bolstered by the fact that the Privacy Policy also states: "We do not share your personal information with third parties for their own direct marketing purposes." Ex. 17 at 6. Thus, the conduct here is directly contrary to the representations in the Privacy Policy.

The purported June 17, 2024 Privacy Policy does not change the analysis (MTD at 16) because there is still no explicit notification by BlueChew that it will share health information with Meta via the Facebook Tracking Pixel. Indeed, under the heading "Medical Information and Providers," BlueChew states: "You will also be required to complete a medical profile where you will communicate health-related information to BlueChew, which we will pass through to the healthcare provider licensed to practice medicine in your jurisdiction . . ." Ex. 19 at p.2. The Privacy Policy says nothing about BlueChew passing protected health information to Meta. As such, Defendant fails to demonstrate that any Plaintiff consented to the conduct at issue here at any time.

Finally, although the FAC does not allege whether Plaintiffs are Facebook users, Defendant contends that if they are Facebook users, Meta's terms (which are not even before the Court) establish consent. MTD at 16 n.7. But Meta has provided no evidence that any of its alleged policies "explicitly notify" Plaintiffs of the fact that it is intercepting sensitive data, including Plaintiffs' protected health information, from third party webpages. *See In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 793-94 (N.D. Cal. 2022) ("I am skeptical that a reasonable user who viewed Meta's policies would have understood that Meta was collecting protected health information.").

C. Plaintiffs' California and Pennsylvania Claims Are Adequately Pled

1. Plaintiffs' CIPA and WESCA Claims Are Not Barred By The Statutes of Limitations Because the Discovery Rule Applies and Because The Statutes of Limitations Are Tolled Due to Defendant's Fraudulent Concealment.

The statute of limitations is an affirmative defense pursuant to which a claim may only be dismissed as time-barred if it "appears beyond doubt that the plaintiff can prove no set of facts that would establish . . . timeliness." *Von Saher v. Norton Simon Museum of Art at Pasadena*, 592 F.3d 954, 969 (9th Cir. 2010); *accord Est. of Gorg v. Great Am. Ins. Co. of Cincinnati Ohio*, 2012 WL 3011728, at *1 (M.D. Pa. May 25, 2012), *report and recommendation adopted sub nom. Est. of Late Gorg v. Great Am. Ins. Co. of Cincinnati Ohio*, 2012 WL 3011726 (M.D. Pa. July 23, 2012) ("The statute of limitations is an affirmative defense and the burden of establishing its applicability rests with the defendant.").

Defendant's argument that Plaintiffs' claims are time-barred fails because of the discovery rule, which "postpones accrual of a cause of action until the plaintiff discovers, or has reason to discover, the cause of action." *Fox v. Ethicon Endo-Surgery, Inc.*, 35 Cal. 4th 797, 806 (2005); *Maier v. Bucks Cnty.*, 2019 WL 689206, at *3 (E.D. Pa. Feb. 19, 2019) ("Pennsylvania law allows for the application of the discovery rule to toll the statute of limitations."); *Gleason v. Borough of Moosic*, 609 Pa. 353, 362-63 (2011) ("The discovery rule applies to toll the statute of limitations in any case in which a party is reasonably unaware of his or her injury at the time his or her cause of action accrued."). Whether the discovery rule applies is generally a "question of fact unless the evidence can support only one reasonable conclusion." *Ovando v. Cty. of Los Angeles*, 159 Cal. App. 4th 42, 61 (2008); *accord Gleason*, 609 Pa. at 362-63 ("The point at which the complaining party should be reasonably aware that he or she has suffered an injury and its cause is ordinarily an issue of fact to be determined by the jury due to the fact intensive nature of the inquiry."). To trigger the discovery rule, a plaintiff need only plead "(1) the time and manner of discovery and (2) the inability to have made earlier discovery despite reasonable diligence." *Fox*, 35 Cal. 4th at 808; *accord SpiriTrust Lutheran v. Wagman Constr., Inc.*, 314 A.3d 894, 906 (Penn. 2024) (to trigger the discovery rule, "the plaintiff must allege facts showing plaintiff's lack of prior knowledge regarding

the nature of the alleged injury, and why plaintiff could not have learned of it at an earlier point").

Plaintiffs' claims are also tolled via equitable tolling. *See Kwai Fun Wong v. Beebe*, 732 F.3d 1030, 1052 (9th Cir. 2013) (applying equitable tolling where delay is due to no "fault of lack of diligence" on behalf of Plaintiff); *accord Deek Inv., L.P. v. Murray*, 157 A.3d 491, 497 (Pa. 2017).

Here, Plaintiffs allege they could not (and did not) discover Defendants' violations despite their due diligence because Defendants had exclusive knowledge of their misconduct, which occurred using proprietary technology that they did not disclose and actively concealed. FAC ¶ 7 ("Due to the surreptitious nature of the interceptions at issue, Plaintiff M.D. did not realize confidential information related to his medical prescription was disclosed to third parties until September 2024."), *id*. ¶ 9 (same for Plaintiff O.F.). Accordingly, Plaintiffs allege the earliest they could have discovered Defendant's violations was in September 2024. *Id.* As Defendant concedes, M.D. filed the initial Complaint in this matter on September 10, 2024, right after Plaintiff M.D. discovered that the unlawful conduct occurred. MTD at 17; Complaint, ECF No. 1. Plaintiffs O.F. and J.P. joined the action by virtue of the FAC on January 6, 2025 (ECF No. 34), well within the applicable statutes of limitations triggered upon discovery in September 2024. *Doe v. Microsoft Corp.*, 2023 WL 8780879, at *5 n.6 (W.D. Wash. Dec. 19, 2023) ("According to the complaint, '[t]he earliest Plaintiff and Class Members could have known about Defendants' conduct was shortly before the filing of this Complaint.' Accepting Plaintiff's allegations as true, the delayed discovery rule tolls the statute of limitations, making the specific timing of alleged misconduct irrelevant to the analysis.").

Defendant argues that Plaintiffs allege they received "advertisements relating to erectile dysfunction medications" following their purchases, which should have put them on inquiry notice of the wrong (MTD at 18), but Plaintiffs do not allege *when* they first began receiving advertisements, which is a question of fact. Regardless, that Plaintiffs saw ads for erectile dysfunction medications does not put them on inquiry notice of Defendant's conduct here because of the surreptitious nature of Defendant's interceptions and the fact that Defendant concealed its conduct from the public. FAC ¶¶ 7, 9. Nor would it be reasonable for Plaintiffs to assume (let alone discover through source code analysis) that their private health information was disclosed by Blue Chew, especially in light of

representations to the contrary. *See* Ex. 17 at 6 ("We do not share your personal information with third parties for their own direct marketing purposes.").

Defendant contends that the BlueChew policies should have placed Plaintiffs on "inquiry" notice of their claims. MTD at 18. That is wrong. Even assuming that Plaintiffs were placed on notice of the BlueChew Privacy Policy, which, for the reasons set forth in Section III.B, *supra*, is a question of fact, BlueChew consistently misrepresented its data sharing practices and even the latest version of its privacy policy does not disclose the widespread, surreptitious health data sharing operation Defendant engaged in. *See* Section III.B., *supra*. Given these misrepresentations, Plaintiffs could not conduct additional diligence (and it would have been futile) because there was no way that an ordinary user could uncover the misconduct Defendant was actively concealing through reading BlueChew's alleged Privacy Policy. *Franklin v. Ocwen Loan Servicing, LLC*, 2018 WL 5923450, at *3 (N.D. Cal. Nov. 13, 2018) (applying discovery rule where plaintiff had no "reason to suspect wrongdoing" because "[t]he very nature of plaintiff's allegations is that the recordings were done surreptitiously."); *Weatherly v. Universal Music Publ'g Grp.*, 125 Cal. App. 4th 913, 919 (2004) ("a defendant cannot hinder the plaintiff's discovery through misrepresentations and then fault the plaintiff for failing to investigate").

In short, suggesting that Plaintiffs were required to compare and contrast (1) the misrepresentations and concealment of the Facebook Tracking Pixel described in the FAC, to (2) vague statements scattered throughout various versions of BlueChew's purported privacy policies (which do not disclose Defendants' conduct (see Section III.B.)), and then (3) perform complex testing to inspect for tracking pixels, would create a heightened and unheard of standard that no court has endorsed. *See Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1071 (N.D. Cal. 2021) (accepting allegations plaintiffs were diligent and finding, in any event, that they "were not obligated to investigate their claims until Plaintiffs had reason to suspect the[ir] existence"); *see also Josten v. Rite Aid Corp.*, 2019 WL 3718739, at *4 (S.D. Cal. Aug. 7, 2019) (explaining a reasonably diligent person would have a "hard time piecing [the misconduct] together" without "having the sophisticated knowledge" of the relevant areas); *In re Ford Motor Co. DPS6 Powershift Transmission Prod. Liab. Lit.*, 2019 WL 6998668, at *3 (C.D. Cal. Sept. 5, 2019) (explaining "[r]easonable diligence does not

require a person to scour the internet in search of any and all information").

The statute of limitations is also tolled by Defendant's fraudulent concealment of its misconduct. This doctrine applies when: "(1) the defendant took affirmative acts to mislead the plaintiff; (2) the plaintiff did not have 'actual or constructive knowledge of the facts giving rise to its claim'; and (3) the plaintiff acted diligently in trying to uncover the facts giving rise to its claim." *Brown*, 525 F. Supp. 3d at 1070; *accord Fine v. Checcio*, 582 Pa. 253, 270 (2005) ("In addition to the discovery rule, the doctrine of fraudulent concealment serves to toll the running of the statute of limitations."); *In re O.E.M./Erie, Inc.*, 405 B.R. 779, 786 (Bankr. W.D. Pa. 2009) (In Pennsylvania, fraudulent concealment "serves to toll the statute of limitations where the wrongdoer has taken some step to deceive, either intentionally or unintentionally, so that the plaintiff is not aware of the injury until after the statute of limitations has lapsed").

Here, Defendant affirmatively acted to mislead Plaintiffs by surreptitiously intercepting Plaintiffs' protected health information while failing to disclose that it collected sensitive health data from third-party web pages (such as BlueChew's website). *See* FAC ¶ 25 ("At no point during the checkout process are patients alerted that information related to their prescription medication is being intercepted by third parties."); *id*. ¶ 13 (Defendant "committed the interceptions at issue without Plaintiffs' knowledge, consent, or express written authorization"); *id*. ¶ 106. Defendant also published misleading Business Tools terms, which suggested that Defendant would not use its technology to intercept sensitive health information, when in fact it does. S*ee In re Glumetza Antitrust Litig.*, 611 F. Supp. 3d 848, 863 (N.D. Cal. 2020) (applying doctrine of fraudulent concealment where defendant made "[H]alf-truths" that omitted information "necessary to prevent misleading others."); *Brown*, 525 F. Supp. 3d at 1070 (holding that defendant's "misleading partial disclosure[s]" were "affirmative acts to mislead Plaintiffs"). As a result, Plaintiffs could not and did not have knowledge of Defendant's conduct despite their diligence to uncover it. *See, e.g.,* FAC ¶¶ 13, 25.

For the foregoing reasons, Plaintiffs M.D. and O.F.'s claims are not barred by the statute of limitations.

2. The Facebook Tracking Pixel is a "Device" Under Both CIPA and WESCA.

Defendant argues that the Facebook Tracking Pixel "is not a 'device' within the meaning of" CIPA and WESCA. MTD at 19. That is wrong. Numerous courts in this District have determined that software, including the Facebook Tracking Pixel, is a "device" under CIPA § 632(a), and Defendant has provided no reason for this Court to deviate from those decisions. *Libman v. Apple, Inc.*, 2024 WL 4314791, at *13 (N.D. Cal. Sept. 26, 2024) ("Plaintiffs have plausibly alleged that the Apple Apps at issue in this case constitute a 'device' under Section 632."); *Meta*, 690 F. Supp. 3d at 1080 ("I agree that the Pixel software is a device under section 632(a)."); *Yockey v. Salesforce, Inc.*, 745 F. Supp. 3d 945, 955 (N.D. Cal. 2024) ("The Court agrees with those Ninth Circuit district court decisions that have found that software qualifies as a device under Section 632.").

While CIPA does not define "device," courts routinely look to the Federal Wiretap Act for guidance. *Gladstone*, 739 F. Supp. 3d at 856. "The majority of courts to consider this issue" under the Federal Wiretap Act and analogous state wiretapping laws, including CIPA § 632, "have entertained the notion that software may be considered a device for the purpose of the Wiretap Act." *United States v. Hutchins*, 361 F. Supp. 3d 779, 795 (E.D. Wis. 2019) (collecting cases); *see also Gladstone*, 739 F. Supp. 3d at 856 ("[T]he Court finds that 'device,' as used in Section 632, can include software."); *Meta*, 690 F. Supp. 3d at 1080 ("I agree that the Pixel software is a device under [CIPA] section 632(a)."); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1084 (N.D. Cal. 2015) ("Plaintiffs have sufficiently alleged that the Carrier IQ Software is a 'device' for purposes of the Wiretap Act."); *Luis v. Zang*, 833 F.3d 619, 634 (6th Cir. 2016) (holding plaintiff plausibly alleged that computer software was "a device … primarily useful for [] the surreptitious interception of [] electronic communications" under Federal Wiretap Act) (cleaned up).

Courts interpreting the definition of "device" under WESCA have held the same. *James v. Walt Disney Co.*, 701 F. Supp. 3d 942, 957-58 (N.D. Cal. 2023), *motion to certify appeal denied*, 2024 WL 664811 (N.D. Cal. Feb. 16, 2024) (denying motion to dismiss WESCA claim where the defendant argued software was not a "device"). WESCA defines "device" as follows:

> **"Electronic, mechanical or other device."** Any device or apparatus, including, but not limited to, an induction coil or a telecommunication

> identification interception device, that can be used to intercept a wire, electronic or oral communication other than:
>
> (1) Any telephone or telegraph instrument, equipment or facility, or any component thereof, furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business, or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business, or being used by a communication common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties.
>
> (2) A hearing aid or similar device being used to correct subnormal hearing to not better than normal.
>
> (3) Equipment or devices used to conduct interceptions under section 5704(15) (relating to exceptions to prohibition of interception and disclosure of communications).

18 Pa. C.S.A. § 5702 (emphasis added). Further, the term "electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system . . . ." *Id.* Clearly, the Facebook Tracking Pixel is a "device or apparatus . . . that can be used to intercept a . . . electronic . . . communication." Plaintiff O.F. alleges several pieces of software that constitute as a "device" under WESCA. FAC ¶ 124. Nothing else is required. *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) ("At the pleading stage, the Court must assume the truth of Revitch's allegation that NaviStone's code is a device … primarily or exclusively designed or intended for eavesdropping upon the communication of another.").

The Third Circuit's decision in *Popa* is instructive. There, the plaintiff alleged that "Navistone intercepted her Personal Identifiable Information ("PII")—her name, her residential address, and her email address—as she browsed HCG's website for pet products," and "that Navistone recorded and relayed her every keystroke and mouse click back to its server." 426 F. Supp. 3d 108, 112 (W.D. Pa. 2019). The court found that (1) whether software code is a "device" is a factual question that "warrants deeper factual exploration than was available at the motion to dismiss stage"; and (2) "[e]xceptions to WESCA's definition of 'devices' must be construed narrowly and none of them seemingly apply" where a defendant is intercepting communications through software code. *Popa*, 426 F. Supp. 3d at 117. Those same findings apply here to Defendant's

Facebook Tracking Pixel. *See Vonbergen v. Liberty Mut. Ins. Co.*, 705 F. Supp. 3d 440, 455 (E.D. Pa. 2023) ("Notwithstanding this apparent inclusivity [of the definitions of "device" under WESCA], Liberty Mutual invites the Court to find that software, including session replay software, cannot constitute a 'device' under the Pennsylvania Wiretap Act as a matter of law. The Court declines the invitation."); *see also id.* at 456 (collecting cases and noting that "many courts to have considered the issue agree that software can constitute a 'device' under the Pennsylvania Wiretap Act and similar anti-wiretapping statutes").

Defendant seeks to impose a limitation that a "device" is limited to "tangible objects." MTD at 20. For WESCA, the court in *Vonbergen* rejected the same argument, holding, "the Court declines to find a 'tangibility' requirement for devices under the Pennsylvania Wiretap Act." *Vonbergen*, 705 F. Supp. 3d at 455.

Courts interpreting CIPA have rejected similar tangibility arguments. As one court noted:

> [Defendant's] position is problematic because it ignores the fundamental fact that, in order for software to work, it must be run on some kind of computing device. It is artificial to claim that software must be viewed in isolation from the computing device on which it runs and with which it is inseparable in regard to the challenged conduct.

James, 701 F. Supp. 3d at 958; *see also Rodriguez v. Ford Motor Co.*, 722 F. Supp. 3d 1104, 1115 (S.D. Cal. 2024) ("It is not apparent to this Court why the statutory language would 'undeniably' apply to a computer but not the software that a computer entails."). In other words, accepting Defendant's argument would mean divorcing the Facebook Tracking Pixel software from the physical, tangible computer the software is running on. Such an interpretation flies in the face of the California Supreme Court's directive to apply CIPA "to new technologies where such a reading would not conflict with the statutory scheme." *Matera v. Google Inc.*, 2016 WL 8200619, at *20 (N.D. Cal. Aug. 12, 2016).

Defendant relies on *Moreno v. San Francisco Bay Area Rapid Transit Dist.*, 2017 WL 6387764, at *5 (N.D. Cal. Dec. 14, 2017), but that case concerned CIPA § 637.7. As courts have recognized, "Section 632 contains materially different language than Section 637.7, and it does not contain similar context that would narrow the meaning of 'device' here." *Gladstone*, 739 F. Supp.

3d at 857; *Tate v. VITAS Healthcare Corp.*, 2025 WL 50447, at *5-6 (E.D. Cal. Jan. 8, 2025). Specifically, CIPA § 637.7(d) defines a device as something "attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals." By contrast, CIPA § 632 was enacted "to be more expansive," and "the Ninth Circuit has observed the California Supreme Court's instruction that all CIPA provisions are to be interpreted in light of the broad privacy-protecting statutory purposes of CIPA." *Gladstone*, 739 F. Supp. 3d at 856 (internal citation and quotation marks omitted); *see also Matera*, 2016 WL 8200619, at *19 ("[W]hen faced with two possible interpretations of CIPA, the California Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest privacy protection."). Thus, decisions citing to CIPA § 637.7—a narrower subsection of CIPA—should not dictate the Court's interpretation of the broader language of CIPA § 632.

3. Meta Was Not a Party to the Communications Between Plaintiffs and BlueChew, It Was an Eavesdropper.

Defendant argues that "Plaintiff M.D.'s CIPA Section 631 claim also fails because, as to the allegedly sensitive information at issue, the [Facebook Tracking] Pixel was merely a tool for BlueChew—a party to the communications." MTD at 20-21.

As an initial matter, whether Defendant is a party to the communication or a third-party eavesdropper is a question of fact not suitable for determination on a motion to dismiss. *Kauffman v. Papa John's Int'l, Inc.*, 2024 WL 171363, at *7 (S.D. Cal. Jan. 12, 2024) ("Whether FullStory acts akin to a tape recorder or whether its actions are closer to 'an eavesdropper standing outside the door' is a question of fact which is better answered after discovery into the session replay technical context of the case."); *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1081 (C.D. Cal. 2021) ("The question thus becomes, in analogue terms: is Quantum Metric a tape recorder held by Lululemon, or is it an eavesdropper standing outside the door? This is a question of fact for a jury, best answered after discovery into the storage mechanics of Session Replay."); *Esparza v. Kohl's, Inc.*, 723 F. Supp. 3d 934, 942 (S.D. Cal. 2024) ("The Court finds here that whether ASI acts akin to a tape recorder or whether its actions are closer to 'an eavesdropper standing outside the door' is a question of fact which is better answered after discovery.").

Regardless, Defendant "intercepted Plaintiff M.D.'s personally identifiable information ("PII"), including his first and last name, email address, and date of birth. Subsequently, as a result of Defendants' conduct, Plaintiff M.D. has received targeted advertisements relating to erectile dysfunction medications." FAC ¶ 8. In short, Plaintiff M.D. alleges that Defendant intercepted his personal information, including his private health information disclosed on the BlueChew website, and used it by incorporating it into its advertising products, as evidenced by Plaintiff M.D. receiving targeted advertising for erectile dysfunction medications. *Id.*; *see also id.* ¶ 40, Figures 5 and 6 (demonstrating that the Facebook Tracking Pixel functions to transmit the full name and contact information of the BlueChew customer as well as the particular prescription medication purchased on BlueChew's website); ¶¶ 41-44. Regardless of whether Plaintiffs are Facebook users, Defendant can match their prescription information "to the specific BlueChew patient based on the PII intercepted from the patient's medical profile." *Id.* ¶ 56. "After collecting and intercepting the information described [herein], Facebook processed, analyzed, and assimilated it into datasets like Core Audiences and Custom Audiences." *Id.* ¶ 57; ¶ 110 ("Defendants utilized Plaintiff M.D.'s and California Class Members' sensitive personal and health information for their own purposes, including for targeted advertising."). Defendant was acting as far more than merely a tool for BlueChew, it was actively intercepting protected health information and using it for its own benefit.

Considering the foregoing, Defendant's argument that somehow its targeting is only limited to Facebook users (MTD at 22) is incorrect. Defendant accesses PII from BlueChew and can match it to specific prescription information, regardless of whether the BlueChew customer is a Facebook user. *Id.* ¶ 56.

4. The First Clause of CIPA § 631(a) Applies to Defendant's Online Wiretaps.

Defendant contends that Plaintiff cannot bring a claim under the first clause of CIPA § 631(a) because "M.D. alleges interception of communications made over the internet only." MTD at 23. Defendant is wrong. In a similar pixel action, Judge Pitts concluded that CIPA applied to the LinkedIn Insight Tag, explaining "Section 631 applies to 'new technologies' such as computers, email, and the Internet." *Jackson v. LinkedIn Corp.*, 744 F. Supp. 3d 986, 993 (N.D. Cal. 2024)

(quoting *Matera*, 2016 WL 8200619, at *20). In *Matera*, the court noted that the "California Supreme Court . . . regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." 2016 WL 8200619, at *20. After surveying California case law applying this principle, the court in *Matera* concluded that "[b]ecause the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme, the Court is unpersuaded by Google's argument that CIPA cannot apply to email because email did not exist at the time of CIPA's enactment." *Id.*

In *Kauffman*, 2024 WL 171363, at *8, the court applied *Matera* and reasoned that "[r]eading the first clause of Section 631 to apply only to communications through a wire ignores the fact that a statute may be read to apply to new technologies . . ." *See also id.* ("[t]hough written in terms of wiretapping, § 631(a) applies to internet communications") (quoting *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *2 (9th Cir. May 31, 2022)). Plaintiff alleges that "Defendants, through their SDKs and other software code, intentionally tapped or made unauthorized connections with the lines of internet communications between Plaintiff M.D. and California Class Members and the Website without the consent of all parties to the communication." FAC ¶ 96. Plaintiffs therefore adequately pleads a violation of the First Clause of CIPA.

5. Plaintiff M.D. States a Claim for Invasion of Privacy under the California Constitution Because Defendant's Conduct in Intercepting Plaintiff's Private Health Information Without Consent Was Highly Offensive.

To state a claim for invasion of privacy under the California Constitution, Plaintiff "must show that (1) [he] possess[es] a legally protected privacy interest, (2) [he] maintain[s] a reasonable expectation of privacy, and (3) the intrusion is 'so serious ... as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020) (quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009)). Here, Defendant challenges only the third element. *See* MTD at 23 ("Plaintiff M.D.'s California invasion of privacy claim also fails because Plaintiffs' allegations that *BlueChew* sent sensitive data to Meta fail to show that *Meta* committed any highly offensive intrusion, as required by California law.").

Here, Defendant's conduct was highly offensive. As a threshold matter, "questions of whether conduct is 'egregious,' 'offensive,' or violates 'social norms' tend by their very nature to be subjective . . . [and] these questions are typically more appropriately resolved by a jury." *Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1139 (E.D. Cal. 2021); *see also In re Google Location Hist. Litig.*, 514 F. Supp. 3d 1147, 1157 (N.D. Cal. 2021) ("Whether [defendant's] collection and storage of location data when Location History was set to off was highly offensive to a reasonable person is a question of fact.") (citing *Facebook Internet Tracking*, 956 F.3d at 606). Indeed, the Ninth Circuit held that this determination "requires a holistic consideration of factors" and raises "an issue that cannot be resolved at the pleading stage." *Facebook Internet Tracking*, 956 F.3d at 606.

Here, Plaintiff M.D. has identified sufficient facts to survive a motion to dismiss because he pleads that Defendant surreptitiously collected his private health information in unexpected ways. Indeed, under similar circumstances, the court in *In re Meta Pixel Healthcare Litig.* found:

> There is support for plaintiffs' position that Meta has behaved egregiously. By enacting criminal and civil statutes forbidding the disclosure of protected health information without proper authorization, Congress has made policy decisions regarding the importance of safekeeping this information. *See, e.g.*, 42 U.S.C. § 1320d-6 (providing criminal and civil penalties for disclosing protected health information without authorization); 45 C.F.R. § 164.508 (requiring a "valid authorization" for use or disclosure of protected health information). Courts have also found that taking personal contact information without consent could be deemed highly offensive. *See Opperman v. Path*, 87 F. Supp. 3d 1018, 1060–61 (N.D. Cal. 2014) (finding that a jury must decide whether the "surreptitious theft of personal contact information" is highly offensive). Finally, I note that Meta's policies forbid the transmission of health-related information, which the Ninth Circuit has found to be relevant in the "highly offensive" inquiry. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 606 (finding that highly offensive element was sufficiently pleaded where Facebook collected full-string detailed URLs and where "Plaintiffs have alleged that internal Facebook communications reveal that the company's own officials recognized these practices as a problematic privacy issue."). These arguments have merit.

647 F. Supp. 3d at 800-01; *see also M.G.*, 2024 WL 4219992, at *6 (Martínez-Olguín, J.) (egregious nature of similar conduct raises "a factual dispute and Headway has not met its burden to show that

the information disclosed here – M.G.'s provider preference, appointment details, and search concerning mental health conditions – cannot allege a serious invasion of privacy").

The same analysis applies here. Plaintiff M.D. disclosed private health information when interacting with the BlueChew Website, including the purchase of erectile dysfunction medication, which is entitled to stringent protections under federal law. Further, Defendant purports to forbid the transmission of health-related information using the Facebook Tracking Pixel through its Business Tools terms (although, in practice, it does not), which reveals that Defendant's own officials recognize that collection of such data is a problematic privacy issue.

Defendant raises issues of fact, namely that "Plaintiffs do not allege that *Meta* served them targeted advertisements, nor do they plausibly allege that Meta ever used their personally identified purchase information for *any* of its own purposes." MTD at 24. That is wrong because Plaintiff M.D. alleges, "as a result of Defendants' conduct, Plaintiff M.D. has received targeted advertisements relating to erectile dysfunction medications." FAC ¶ 8; *see also* ¶ 5 ("Defendants intentionally targeted and used this information for their own purposes, including for targeted advertising."). Defendant's conduct in surreptitiously intercepting Plaintiff M.D.'s private health information—pertaining to the purchase of erectile dysfunction medication—to use for its own advertising purposes is highly offensive. At minimum, a reasonable jury could conclude that it is highly offensive. Therefore, Defendant's motion to dismiss Plaintiff M.D.'s claim of invasion of privacy under California's Constitution should be denied.

IV. CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that the Court deny Defendant's Motion to Dismiss. If the even the Court concludes that any portion of Plaintiffs' FAC is deficient, Plaintiffs seek leave to cure any such deficiencies.

Dated: April 7, 2025

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ L. Timothy Fisher*
L. Timothy Fisher

L. Timothy Fisher (State Bar No. 191626)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: ltfisher@bursor.com

Counsel for Plaintiffs